March 8, 2006

STATEMENT OF ROBERT SCAVONE,

EXECUTIVE VICE PRESIDENT,

P&O PORTS NORTH AMERICA, INC.

BEFORE THE HOUSE SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

Mr. Chairman and Members of the Committee,

My name is Rob Scavone. I am Executive Vice President of P&O Ports North America, Inc. Among my responsibilities is the supervision of our compliance with security requirements in the U.S. I am a member of the Board of Directors of the National Association of Waterfront Employers, or "NAWE" an association of marine terminal operators in the U.S., both American and foreign. I also serve as co-chairman of an advisory group to the International Standards Organization on matters of container security, which group includes all major international terminal operators.

The Subcommittee has asked for testimony concerning the ongoing implementation of several programs related to cargo security, and I thank you for the opportunity to submit my comments on those matters here today.

Transportation Worker Identification Credentialing

The most anticipated program from my perspective, among those that are pending, is the Transportation Worker Identification Credential, or "TWIC" program. We in the terminal operating side of the industry are well aware that this project has been slow in gestation, but we also recognize that the TWIC rulemaking is a substantial and complex undertaking. We are mindful of the fact that the procedures required in a final TWIC rule must work in conjunction with our terminal operating gate systems, and we have strived to work with the agencies to minimize problems with the TWIC when it is implemented. We further understand that challenges exist with respect to the technology for scanning the cards, and recording biometric data.

It is now our understanding that the target date for issuing a Notice of Proposed Rule Making for the TWIC program is now around July 1st. We are also aware that, in view of the delays that have occurred to the implementation of this program, some have proposed interim measures, such as immediate worker background checks, to be performed by the employers. We, as much as anyone, understand the sense of frustration with the extended timetable for this program. We ourselves have forestalled the installation of other identification-based access controls, in anticipation of this program. However, we strongly suggest that the insertion of the employer between the government and the

transport worker for the purpose of background checks will be counterproductive. The employers simply do not have the resources, capabilities, or access to information that the government has. More importantly, many of the workers who will require ID cards, such as truckers, are themselves owner-operators, with no employer other than themselves, and unrelated to the terminal operator. We urge this Subcommittee to encourage TSA to continue on the current path to finalize the TWIC program.

In terms of specific features, it must be recognized that the response time for a transaction with a TWIC card at our gates must be several seconds, at most. This argues against the use of a central national database. This may not be a significant problem, since most of the persons entering our gates, including truckers, would be local and repetitive, but it begs the question as to how much of the responsibility for hosting and supporting the data base should fall on the terminal operator. Clearly the terminal operator cannot be responsible to keep the data current, for example. And the terminal operator should not be responsible to host a substantial amount of such data on its own computer hardware in order to make the system work.

Security of the Global Supply Chain

Over recent times, we have become accustomed to hearing that our ports in the U.S. are the "most vulnerable" points of entry. This, in turn, tends to lead to the incorrect conclusion that the ports themselves are the *location* where security needs most to be enhanced. This is not correct. Our ports in the U.S. are *already* the one point in the supply chain over which we have the *most* control.

The main point is that, if the security of the supply chain *in a foreign location* should fail, the place where we in the U.S. will be first *exposed* to that failure would, of course, be in the U.S. port. However, no amount of security on the part of the terminal operator in that U.S. facility will change that.

Therefore, the enhancement of the security of our U.S. ports, and, by extension, our homeland, is best accomplished by improving the security at the point of origin. Of course, this concept is not new, and in fact such programs as the 24-hour rule, C-TPAT, and the CSI program, have all contributed to this goal. However, if efforts will be made to continually improve our security, this is where the focus must remain.

Such efforts will be focused upon such matters as: the integrity of container seals; improved capability to conduct non-intrusive inspections at the port of loading; upgrading of the Automated Targeting System; greater cooperation between U.S. Customs and the local customs officials; and related technologies to permit better tracking of cargo loads along the supply chain.

Some of these objectives will experience substantial progress via the simple decision to devote more resources to them. We in the industry urge this Subcommittee to do its part to see that this happens. Others will require a global, comprehensive government-

industry effort, which will include the governments of virtually every trading country, and both carriers and marine terminal operators, together with technology vendors, and international standards bodies such as ISO, the International Standards Organization.

Foreign Ownership

The fact that foreign interests own many of the companies that manage our terminals in the U.S. has recently become a major point of discussion. The focus has been on the extent to which such ownership may impact the security function inside our terminals. The answer is, it does not impact the security function at all, for the following reasons:

1. The Coast Guard and Customs continue to be responsible for all security measures relating to the entrance of persons or goods into the United States. Those agencies maintain a presence in the ports, and work with the Port and local police. Our terminals work in close cooperation with those authorities every day. The statement that the security of our ports is being outsourced is simply not the case.

2. Inside a terminal, only longshoremen perform any physical work on containers. By way of example, P&O Ports employs approximately 6000 longshoremen every day.

3. The terminal operator has no role in verifying or inspecting the declared contents of any container entering the United States. In fact, the terminal operator does not request from the carrier, nor does it require, any information concerning the contents, origin, or destination of the containers that it handles, unless, of course the cargo is declared to be hazardous, because those containers have separate handling procedures. That role is performed exclusively by U.S. Customs. No container leaves a U.S. facility until U.S. Customs indicates that it is free to go.

4. When Customs decides which containers will be opened, they do it with their own staff, not with the terminal operator's workers.

Mr. Chairman, thank you very much for the opportunity to provide these remarks today.